(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 41 862 A 1**

(51) Int. Cl.[7]:
G 07 F 7/08
G 06 F 15/02
H 04 M 1/00

(21) Aktenzeichen: 198 41 862.0
(22) Anmeldetag: 14. 9. 1998
(43) Offenlegungstag: 16. 3. 2000

(71) Anmelder:
Wieland, Andreas W., 57076 Siegen, DE

(72) Erfinder:
Wieland, Andreas W., 57076 Siegen, DE; Müller, Maik, 57223 Kreuztal, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 34 12 663 A1
EP 07 90 587 A1
WO 96 32 700 A1
WO 92 11 598 A1

RANKL,W., EFFING,W.: Smart Card Handbook, John Wiley & Sons, New York, u.a., 1997, S.342-347;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Inegration von Chipkartenfunktionen in ein mobiles Kommunikationsgerät

(57) Die Erfindung "Integration von Chipkartenfunktionen in ein mobiles Kommunikationsgerät" soll wesentliche Nachteile von Chipkarten, insbesondere verschiedene Sicherheitsprobleme, dadurch lösen, daß die Funktionalität von Chipkarten in ein elektronisches Transaktionsgerät, also ein Mobiltelefon, einen elektronischen Organizer etc. integriert wird. Dabei kann die Chipkartenanwendung von Hard- und/oder Software Gebrauch machen, über die dieses Transaktionsgerät ohnehin verfügt. Dieses Transaktionsgerät kann für die Chipkartenanwendungen mit zusätzlichen Sicherheitsmodulen ausgestattet werden. Die Vorteile liegen auf der Hand: Das Transaktionsgerät verfügt über eigene Benutzerschnittstellen, so daß der Benutzer nicht mehr dem Chipkarten-Anwendungsterminal vertrauen muß. Das Transaktionsgerät verfügt über eine eigene, autarke Stromversorgung. Der wesentliche Vorteil jedoch ist, daß das Transaktionsgerät über mehr Rechenleistung als jede bekannte Chipkarte verfügt. Mit dieser Rechenleistung ließen sich starke kryptographische Verfahren zur Sicherung von Chipkartenanwendungen einsetzen, so daß diese Anwendungen in einer Weise sicher gemacht werden können, wie sie bisher unbekannt war.

DE 198 41 862 A 1

DE 198 41 862 A 1

Beschreibung

Die Erfindung betrifft ein Gerät entsprechend dem Oberbegriff des Anspruchs 1.

Es ist bekannt, daß Magnet- und Chipkarten (Smart Cards) (Für Magnet- als auch Chipkarten wird im folgenden Text der Oberbegriff "Karte" verwendet.) heuzutage viele Anwendungen haben, deren Anzahl stetig wächst [1]. Als Beispiele für mögliche oder existierende Anwendungen seien (ohne Anspruch auf Vollständigkeit) die folgenden genannt: Elektronische Zugangskontrollsysteme, Bankkarten (zur Verwendung z. B. in Kontoauszugdruckern oder Geldautomaten oder als Bargeldkarten), elektronische Authentikationssysteme, (Kranken-) Versicherungskarten, Telephonkarten, Karten zur sicheren Personalisierung von Mobiltelephonen etc. In allen genannten und den meisten anderen Anwendungen ist die Sicherheit ein wichtiger Faktor im Hinblick auf die Einsetzbarkeit der Karte. Dabei bedeutet Sicherheit in den allermeisten Fällen, daß die Karten nicht fälschbar oder manipulierbar sein dürfen und daß nur der rechtmäßige Karteninhaber diese benutzen können darf; im Falle eines Verlustes oder gar Diebstahls der Karte sollte deren Benutzung für dritte Personen unmöglich sein [1, S. 258 ff.]. Außerdem sollte sichergestellt sein, daß die Karte nur in der vom Benutzer bzw. Diensteanbieter beabsichtigten Weise verwendet wird, d. h. nur vom Benutzer gewollte bzw. vom Diensteanbieter erlaubte Transaktionen sollen durchgeführt werden.

Im folgenden soll zunächst dargestellt werden, wie Kartenanwendungen prinzipiell arbeiten; diese Darstellung ist verallgemeinert und kann im Einzelfall anders aussehen, weshalb für detaillierte Informationen auf [1] verwiesen sei.

Magnetkartenanwendungen

Prinzipiell folgt der Ablauf einer Magnetkartenanwendung dem folgenden Schema:

1. Der Benutzer schiebt seine Magnetkarte in das Kartenterminal.
2. Die Karteninformation wird gelesen und es wird überprüft, ob die darauf enthaltenen Daten konsistent sind.
3. Das Terminal fordert den Benutzer auf, sein Authentikationsgeheimnis einzugeben. Dieses Authentikationsgeheimnis ist in den allermeisten Fällen eine Persönliche Identifikationsnummer (PIN), es kann aber in Einzelfällen auch ein Paßwort bzw. ein Paßsatz (engl. Password bzw. Pass Phrase) sein. (Grundsätzlich ist Paßwörtern oder gar ganzen Sätzen der Vorzug zu geben, da diese leichter zu merken sind und aufgrund des größeren Zeichenvorrats einen größeren Paßwortraum ermöglichen. Der Einführung dieser alphanumerischen Authentikationsgeheimnisse steht jedoch die Tatsache entgegen, daß die allermeisten heute installierten Kartenterminals nur über numerische Tastaturen verfügen. Vgl. [1, S. 259].)
4. Das Terminal überprüft, ob das Authentikationsgeheimnis und die Karteninformation zusammengehören. Wenn ja, wird mit dem nächsten Schritt fortgefahren, ansonsten können Schritt 3 und 4 wiederholt werden. Die Anzahl der Fehleingaben ist in den meisten Fällen beschränkt (z. B. maximal 3 Fehleingaben). Es gibt jedoch auch Anwendungen, in denen auf diese Abfrage des Authentikationsgeheimnisses verzichtet werden kann. (Als Beispiel seien Zugangssicherungssysteme genannt, in denen die Karte wie ein Schlüssel eingesetzt wird. Dabei wird vorausgesetzt, daß allein der Besitz der Karte, ohne das Wissen um ein Authentikationsgeheimnis, zur Transaktion berechtigt.)
5. Wenn die Authentikation in Schritt 4 erfolgreich war, können nun Transaktionen an dem Terminal durchgeführt werden. Dazu können weitere Benutzereingaben nötig sein (z. B. Geld am Bankautomaten abheben), das muß aber nicht so sein (z. B. automatisches Türöffnen in Zugangssicherungssystemen).
6. Wenn der Benutzer seine Transaktionen abgeschlossen hat, wird die Benutzung des Terminals abgeschlossen und die Karte wieder ausgeworfen. Dabei kann das Terminal noch Informationen über die Kartenbenutzung (z. B. letztes Benutzungsdatum, Anzahl der Fehlversuche bei der Authentikation usw.) auf die Magnetkarte zurückschreiben.

Chipkartenanwendungen

Die Benutzung einer Chipkarte unterscheidet sich von Magnetkartenanwendungen (wenngleich dies für den Benutzer unbemerkt geschieht). An dieser Stelle muß man klar zwischen Speicherchipkarten und Prozessorchipkarten unterscheiden: Speicherkarten werden rein zur Speicherung von Daten verwendet (z. B. Krankenversichertenkarte). Sie bieten im Vergleich zur Magnetkarte den Vorteil, daß sie durch eine zusätzliche Sicherheitslogik – bereichsweise oder ganz – nichtbeschreibbar ausgeführt werden können, wodurch unerwünschte Manipulationen unterbunden werden. Ein anderes Beispiel ist der Einsatz von Speicherkarten als Debitkarten (etwa Telephon-Guthabenkarte). Hier speichert die Karte einen bestimmten Wert, der aufgrund des Aufbaues der Karte nur vermindert, aber nicht erhöht werden kann.

Im Gegensatz zu den sehr einfachen Speicherkarten verfügen Prozessorkarten über eigene Rechenleistung ("Eigenintelligenz"), aufgrund derer auch komplexe Anwendungen realisiert werden können, z. B. kryptographisch sichere Authentikation. Die Verwendung von reinen Speicherkarten läuft nach folgendem Grobschema ab (bei speziellen Anwendungen können Abweichungen von diesem Schema auftreten):

1. Der Anwender steckt die Karte in das Chipkartenterminal. Damit wird die Karte mit Strom versorgt und kann so aktiv werden.
2. Das Terminal liest die auf der Karte enthaltene Information. Dabei kann auch eine einfache Authentikation der Karte stattfinden.
3. Abhängig von den gelesenen Daten können nun Transaktionen durchgeführt werden. Bei Telephonkarten etwa wird dem Benutzer gestattet zu telephonieren, sofern das auf der Karte enthaltene Restguthaben ausreichend ist.
4. Ggf. übermittelt das Terminal der Karte Daten, die diese dann abspeichert. Bei Telephonkarten etwa wird der interne Zähler um den vom Terminal angegebenen Betrag vermindert.
5. Nach Benutzung wird die Karte wieder ausgeworfen.

Bei der Benutzung einer Prozessorchipkarte kann eine starke Authentikation der Karte durchgeführt werden, da sie über eigene Rechenleistung verfügt und außerdem ein Geheimnis speichert, welches sie niemals preisgibt und mit Hilfe dessen sie ihre Identität beweist:

1. Der Benutzer steckt die Karte in das Chipkartenter-

minal. Damit wird die Karte mit Strom versorgt und kann so aktiv werden.

2. Die Karte ist zwar aktiviert, aber noch nicht benutzbar, da sich der Benutzer erst gegenüber seiner Karte (nicht gegenüber dem Terminal, wie bei Magnetkarten!) authentifizieren muß. Weil aber die Karte über keinerlei Benutzerschnittstellen (z. B. Tastatur, Anzeige, Erkennung physischer Merkmale des Benutzers – etwa von Fingerabdrücken) verfügt, muß der Benutzer sein Authentikationsgeheimnis (z. B. Pin, Paßwort) in das Terminal eingeben. Dieses übermittelt das Benutzer-Authentikationsgeheimnis an die Chipkarte.

3. Die Chipkarte prüft diese Information; ist sie korrekt, ist die Chipkarte vollständig aktiv. Chipkarte und Terminal können sich nun gegenseitig ihre Identität beweisen. Dieser Identitätsbeweis kann auf verschiedene Weisen erbracht werden, die Liste erhebt keinen Anspruch auf Vollständigkeit (vgl. [2] bzw. [3]):

- digitale Signaturen
- asymmetrische kryptographische Verfahren (z. B. RSA-Algorithmus)
- ISO-Authentikationsprotokolle
- Zero-Knowledge-Protokolle.

4. Aufgrund des erbrachten Identitätsbeweises hat nun das Terminal die Kontrolle über alle verfügbaren Chipkartenfunktionen, da es als Mittler zwischen Benutzer und Chipkarte auftritt.

5. Auch hier können nach Abschluß aller Transaktionen wieder Informationen über die Kartenbenutzung an die Karte übergeben werden, die diese dann abspeichert. Danach wird die Karte ausgeworfen.

In einigen Anwendungen können die Schritte 2 und 3 auch in umgekehrter Reihenfolge ausgeführt werden, vgl. [1, S. 260].

Schwächen dieser Verfahren

Die vorgenannten Verfahren haben einige immanente Schwächen. Im einzelnen müssen folgende Nachteile genannt werden:

1. In Schritt 2 und 3 der Magnetkartenanwendung gibt der Benutzer sowohl die Karteninformation als auch sein Authentikationsgeheimnis (i. a. die PIN) dem Kartenterminal preis. Damit steht dem Mißbrauch der Karte nichts entgegen: Durch Manipulation des Kartenterminals können die Karteninformation und das Authentikationsgeheimnis abgehört werden. Danach kann ein Kartenbetrüger die Karteninformation auf eine andere Magnetkarte duplizieren und diese wie eine "echte" Magnetkarte verwenden. Eine Variante dieses Angriffs mit einem Trojanischen Pferd wurde vor Jahren von Kreditkartenbetrügern durchgeführt. Diese hatten vor einen echten Geldautomaten eine Atrappe montiert. Der Bankkunde steckte seine Karte in den Leserschlitz der Atrappe und bekam einen täuschend echt aussehenden Benutzerdialog vorgegaukelt. Nachdem der Kunde seine PIN eingetippt hatte, behielt die Attrappe die Karte mit Hinweis auf einen Kartendefekt, wodurch die Betrüger im Besitz der Karte und der dazugehörenden PIN waren. Da bei diesen Angriffen die rechtmäßigen Besitzer vollkommen arglos sind, können sie ihre Magnetkarten erst sperren, wenn der Schaden bereits eingetreten ist. Vgl. auch [1, S. 259 ff.]

2. Derselbe Angriff läßt sich auch mit einem Chipkartenterminal durchführen, allerdings läßt sich hier nur das Authentikationsgeheimnis des Benutzers abhören, da ja die Chipkarte ihr Identifikationsgeheimnis nicht preisgibt. Potentielle Betrüger müssen sich also (z. B. durch Diebstahl) in den Besitz der echten Karte bringen, um diese mißbrauchen zu können.

3. Die beiden vorgenannten Beispiele setzen voraus, daß der Benutzer auf die Integrität des Kartenterminals vertraut. Ist diese Voraussetzung nicht erfüllt, bieten beide Kartenvarianten keine ausreichende Sicherheit, da, wie unter Schritt 2 der Chipkartenbenutzung erläutert, auch hier das Terminal als Mittler zwischen Karte und Benutzer fungiert und somit die volle Kontrolle über die Karte hat. Der Benutzer sieht nur die Informationen über die durchgeführten Transaktionen, die das Terminal ihm anzeigt. Einen Kartenmißbrauch könnte er nicht sehen, da das Terminal einen Mißbrauch kaum anzeigen würde. Ein solcher Angriff könnte praktisch etwa folgendermaßen aussehen: Ein Benutzer möchte mit seiner Geldkarte in einem Kaufhaus eine Hose für 129,90 DM bezahlen. Das (manipulierte) Terminal zeigt einen ganz normalen Benutzerdialog an, in dem dem Kunden mitgeteilt wird, daß von seiner Karte 129,90 DM für diese Hose abgebucht werden. Unbemerkt vom Benutzer bucht das Terminal aber einen weiteren bzw. höheren Betrag ab. Der Benutzer hat keine Möglichkeit, dies zu erkennen, da das Terminal diese Transaktion nicht anzeigt und der zusätzlich abgebuchte Betrag natürlich nicht auf irgendwelchen ausgedruckten Belegen erscheint. Der Benutzer kann dies frühestens bemerken, wenn er bei der nächsten Benutzung seiner Geldkarte feststellt, daß diese einen Fehlbetrag aufweist. Im Gegensatz zu einer Kreditkarte hat er auch keine Möglichkeit, eine Abrechnung anzufechten, da der Geldbetrag direkt von seiner Karte abgebucht wurde und nicht von dem Ladenbesitzer mit einem Kreditkartenunternehmen abgerechnet wird. Mit anderen Worten: Er hat keine nachträgliche Möglichkeit zu beweisen, daß das Geldkartenterminal einen zu hohen Betrag abgebucht hat, außer daß er die Manipulation des Terminals beweist, was dem Normalbenutzer praktisch unmöglich sein dürfte. Erfolgversprechend ist dieser Angriff insbesondere dann, wenn der illegal abgebuchte Betrag so klein ist, daß er unbemerkt bleibt.

Die Sicherheit von Kartenanwendungen hängt aber noch von anderen, wesentlichen Einflüssen ab:

Sicherheitsmechanismen

Die Sicherheitsmechanismen vieler derzeit verwendeter Karten sind schwach im Vergleich zum technisch Möglichen. Dieser Mangel ist dadurch bedingt, daß starke Sicherheitsmechanismen kryptographisch starke und damit mathematisch aufwendige Algorithmen erfordern, was aber Karten mit hoher eigener Rechenleistung bedingt. Solche Karten sind vergleichsweise teuer, weshalb gerade in Massenanwendungen ein Großteil der möglichen Sicherheit zugunsten einer kostengünstigen Realisierung geopfert wird. Insbesondere sind heutige Karten nicht in der Lage, Schlüssel selbst zu generieren; üblicherweise werden Schlüssel bei der Personalisierung der Karte von außen in die Karte geladen [1, S. 322 ff.].

Sicherheitsbewußtsein des Benutzers

Derzeit werden Karten meistens durch ein Benutzer-Authentikationsgeheimnis (z. B. Persönliche Identifikationsnummer, PIN) vor der Benutzung durch Unbefugte ge-

schützt. Dabei muß sich der Benutzer zu jeder Karte ein eigenes Authentikationsgeheimnis merken, was ihn bei der Vielzahl der Kartenanwendungen jedoch überfordert. Deshalb tendieren Anwender dazu, dieses Authentikationsgeheimnis entweder auf der Karte selbst oder nur unzulänglich getarnt, z. B. als Telephonnummer in ihrem Telephonregister, irgendwo zu notieren, wodurch diese Sicherheitsfunktion im Falle eines Kartenverlustes praktisch wertlos ist.

Daneben haben Chipkarten den schwerwiegenden Nachteil, daß sie ohne eigene Stromversorgung auskommen müssen und deshalb als nichtflüchtigen, beschreibbaren Speicher einen EEPROM-Speicher besitzen. Dieser Speicher kann nur begrenzt wiederbeschrieben werden; man geht von ca. 10 000 Schreibzyklen aus. Damit ist die Lebensdauer der Chipkarte begrenzt. Außerdem bietet sich einem Angreifer die Möglichkeit, aus dem Stromverbrauch der Karte Rückschlüsse auf die gerade durchgeführte Operation zu ziehen. Dies kann einen Angriff deutlich erleichtern. Außerdem hat man in den meisten Chipkartenstandards den Leistungsverbrauch von Chipkarten begrenzt; dadurch ist aber auch die Rechenleistung der Karte und somit die Stärke der verwendeten kryptographischen Algorithmen begrenzt.

Die Eigenschaften von Karten für Anwendungen mit hohen Sicherheitsanforderungen lassen sich damit direkt aus den o. g. Nachteilen herauslesen:

1. Es kommen nur Chipkarten in Frage, da Magnetkarten nicht über eigene Rechenleistung ("Eigenintelligenz") verfügen.
2. Chipkarten müssen über genügend Rechenleistung verfügen, um auch mathematisch aufwendige kryptographische Algorithmen auszuführen.
3. Chipkarten müssen über Benutzereingabeschnittstellen verfügen, so daß Benutzereingaben direkt (ohne Umweg über ein möglicherweise nicht vertrauenswürdiges Kartenterminal) in die Chipkarte gelangen. Dadurch wird verhindert, daß das Kartenterminal Kenntnis des Benutzer-Authentikationsgeheimnisses oder anderer sicherheitsrelevanter Informationen gewinnt. Diese Benutzereingabeschnittstelle kann auch eine Erkennung physischer Merkmale (z. B. Fingerabruck) des Benutzers sein.
4. Chipkarten müssen über eigene Benutzerausgabeschnittstellen verfügen, so daß der Benutzer direkt (ohne Umweg über ein möglicherweise nicht vertrauenswürdiges Kartenterminal) die Transaktionen verfolgen kann, die zwischen Karte und Terminal ablaufen. Dadurch bleiben ihm keine Transaktionen verborgen.
5. Eine Chipkarte sollte für möglichst viele Anwendungen einsetzbar sein, so daß der Benutzer sich nur ein einziges Benutzer-Authentikationsgeheimnis merken muß. Das hilft zu verhindern, daß der Benutzer dieses Authentikationsgeheimnis notiert.
6. Chipkarten sollten einen konstanten Stromverbrauch haben oder alternativ über eine autarke Stromversorgung verfügen.

Chipkarten, die die o. g. Eigenschaften aufweisen, sind technisch vielleicht realisierbar, haben jedoch den für Massenanwendungen entscheidenden Nachteil, daß sie viel zu teuer wären.

Im Gegensatz dazu verfügen viele Geräte, die man tagtäglich mit sich führt, etwa Mobiltelephone, elektronische Organizer oder sogar leistungsfähige Taschenrechner, über genügend Rechenleistung – die oft sogar nur während eines Bruchteils der Betriebszeit genutzt wird – um solche Chipkartenfunktionen auszuführen. Sie verfügen außerdem über Benutzerschnittstellen in Form einer Tastatur und einer Anzeige und werden von Batterien bzw. Akkumulatoren gespeist.

Die Aufgabe der Erfindung besteht darin, ein Gerät wie ein Mobiltelephon, einen Organizer o. ä. (im folgenden Persönliches Elektronisches Transaktionsgerät, PET genannt) durch Modifikationen/Erweiterungen von dessen Hard- und/oder Software für typische Chipkarten-Applikationen nutzbar zu machen.

Diese Aufgabe wird durch ein Gerät des Anspruchs 1 gelöst.

Das PET verfügt über genügend Rechenleistung, um für Chipkartenapplikationen typische Algorithmen bzw. Programme auszuführen, bzw. Algorithmen bzw. Programme auszuführen, deren Komplexität jene heutiger Chipkartenapplikationen weit übersteigt. Insbesondere ist auch eine (sehr rechenzeitaufwendige) Schlüsselerzeugung im Gerät möglich. Es ist auch in der Lage, mehrere Applikationen zu bedienen. Es verfügt darüberhinaus über Benutzerschnittstellen in Form von Tastatur und Anzeige, sowie meistens über zusätzliche Peripherieschnittstellen. Über die bereits vorhandenen Peripherieschnittstellen oder zusätzlich einzubauende Schnittstellen (z. B. einen Chipkartendummy nach den Ansprüchen 9–16) läßt sich das Chipkartenterminal mit dem PET verbinden. Der Benutzerdialog kann vollständig über das Display und die Tastatur des PET abgewickelt werden, so daß der Benutzer immer die volle physische Kontrolle über die ausgeführten Transaktionen hat. Dadurch werden insbesondere Angriffe mit Hilfe Trojanischer Pferde unmöglich. Bei Verwendung von Challenge-and-Response-Authentikationsprotokollen (auch Challenge-and-Reply-Authentikationsprotokolle genannt) oder Zero-Knowledge-Authentikationsprotokollen kann der Benutzer Transaktionen an Terminals durchführen, denen er zunächst mißtraut, da bei solchen Protokollen keine Authentikationsgeheimnisse ausgetauscht werden. In bestimmten Fällen kann es notwendig sein, das PET mit zusätzlichen Sicherheitsmodulen auszustatten, z. B. um anwendungsspezifische Geheimnisse eines Diensteanbieters vor dem Benutzerzugriff zu schützen.

Dadurch, daß das PET über Tastatur und Anzeige verfügt, lassen sich noch weitere interessante Eigenschaften realisieren. Wünschenswert könnte es beispielsweise sein, wenn man Transaktionen freigeben könnte, während man sich in einer sicheren Umgebung befindet, um diese Transaktionen erst später wirklich durchzuführen. Dazu ein Beispiel: Ein Benutzer möchte nicht, daß sein Authentikationsgeheimnis (z. B. seine PIN) ausgespäht werden kann, während er diese in sein PET eingibt, etwa in einer Warteschlange vor einem Bankterminal oder einem Kassenterminal in einem Kaufhaus. Mit einer sog. Vorfreigabefunktion könnte er sein PET authorisieren, eine Bezahlungstransaktion bis zu einem bestimmten Betrag an einem Terminal durchzuführen, ohne daß er während des eigentlichen Bezahlvorgangs sein Authentikationsgeheimnis eingeben muß. Diese Vorfreigabe könnte beispielsweise in seinem Kraftfahrzeug (eine relativ sichere Umgebung) stattfinden, danach kann der Benutzer im Kaufhaus bezahlen, ohne das Authentikationsgeheimnis neu einzugeben, solange er den vorher angegebenen Betrag nicht überschreitet.

Da das PET außerdem über genügend Speicher verfügt bzw. mit genügend Speicher ausgestattet werden kann, läßt es sich für mehrere Chipkartenanwendungen einsetzen. Die Verwendung von Schlüsselhierarchien bzw. Schlüsseln mit zeitlich begrenzter Gültigkeit [1, S. 279 ff.] wird nicht länger durch den begrenzten Speicherplatz einer Chipkarte eingeschränkt. Die zu jeder Anwendung gehörenden Benutzerauthentikationsgeheimnisse lassen sich dabei in einer kryptographisch geschützten Datenbank ablegen, so daß der Be-

nutzer sich nur noch ein einziges Benutzerauthentikationsgeheimnis statt vieler applikationsspezifischer Benutzerauthentikationsgeheimnisse merken muß. Dies ist aus sicherheitstechnischer Sicht zwar möglicherweise nicht völlig unbedenklich, aber auf jeden Fall besser als auf Karten notierte PINs.

Ein großer Vorteil für Diensteanbieter ergibt sich für den Fall, daß ein Mobiltelephon als PET verwendet wird. Dadurch, daß das Mobiltelephon praktisch dauernd erreichbar ist, kann ein Diensteanbieter die Daten des PET online über eine Telephonverbindung aktualisieren. Diese Möglichkeit wäre beispielsweise interessant für den Fall, daß Schlüssel der Applikation kompromittiert wurden und ausgetauscht werden müssen. Ohne Online-Verbindung müßte der Benutzer seine Karte beim Diensteanbieter abliefern, welcher der Karte entweder neue Schlüssel einprogrammiert oder aber die Karte tauscht. Das ist sowohl für den Benutzer als auch für den Anbieter zeitraubend und aufwendig. Über die Online-Verbindung könnte dieser Schlüsselaustausch stattfinden, ohne daß die Karte dem Diensteanbieter physikalisch zugänglich gemacht werden muß.

Weitere Vorteile ergeben sich für die Hersteller der PETs, speziell allerdings für den Fall, da Mobiltelephone als PET eingesetzt werden. Dadurch daß für Chipkartenanwendungen speziell zertifizierte Betriebssysteme erforderlich sind, müßten auch die Betriebssysteme der PETs entsprechend zertifiziert sein. Dies ist zunächst für den Hersteller mit erheblichem Mehraufwand verbunden, jedoch erhöht sich dadurch die Qualität seines Produktes, was für den Hersteller auch durchaus als Marketingargument verwertbar ist.

In allen vorgenannten Fällen kann es notwendig werden, das PET mit einem oder mehreren zusätzlichen Sicherheitsmodulen, z. B. in Form von Chipkarten, auszustatten, um sensitive Daten besonders zu schützen.

Daneben könnte es interessant sein, die Chipkarten-Kryptofunktionen, die in ein PET integriert werden müssen, auch für andere Anwendungen zu verwenden. Z. B. wäre es denkbar, Telekommunikationsverbindungen besser zu verschlüsseln als es mit den heute in Mobiltelephonen integrierten Algorithmen möglich ist. Verwendet man einen Personal Organizer als PET, ließen sich die zusätzlich integrierten Kryptofunktionen auch für das Signieren und Verschlüsseln von Daten (z. B. eMails) verwenden. Den Anwendungsmöglichkeiten dieser Funktionen sind, dabei kaum Grenzen gesetzt.

Ausführungsbeispiele der Erfindung sind im folgenden beschrieben. Diese Beschreibung ist aufgrund der Vielzahl der Ausführungsmöglichkeiten zweigeteilt, da auch zwei Probleme gelöst werden müssen: Erstens kann die Verbindung zwischen dem PET und dem Anwendungsterminal auf verschiedene Weisen erfolgen. Zweitens kann das PET – je nach Anforderung des Diensteanbieters und des Benutzers – verschiedene Anwendungen bzw. Betriebsmodi unterstützen.

Die physikalische Verbindung zwischen PET und Anwendungsterminal kann über Schnittstellen erfolgen, über die das PET bereits verfügt, etwa die Infrarotschnittstelle eines Personal Organizers oder über den Sendeempfänger eines Mobiltelephons. Für die nähere Zukunft dürften jedoch Chipkartennachbildungen (Chipkartendummies) notwendig sein, um Transaktionen auch an einem der vielen bereits aufgestellten Kartenterminals durchführen zu können.

Bildlich dargestellt ist diese Anordnung in **Abb.** 1. Der Chipkartendummy ist nichts anderes als eine Vorrichtung, die äußerlich wie eine Chipkarte aussieht, die jedoch nur zur Herstellung einer Verbindung zwischen PET und Kartenterminal notwendig ist. Diese kann – je nach technischer Notwendigkeit – über eigene aktive elektronische Komponenten verfügen oder einfach nur eine Kontaktiereinrichtung sein. Die eigentliche Chipkartenfunktion übernimmt das PET, welches hier als Mobiltelephon dargestellt ist. Der Chipkartendummy kann dabei die Nachbildung einer Chipkarte mit mechanischen Kontakten oder einer mit berührungsloser Kontaktierung sein. Damit der Chipkartendummy universell verwendbar ist, sollte er jedoch auf beide Arten kontaktierbar sein. Die Kommunikation zwischen Chipkartendummy und PET kann ebenfalls auf verschiedene Weisen erfolgen. Am einfachsten ist sicher eine Verbindungsleitung realisierbar; jedoch ist diese inkompatibel zu vielen existierenden Chipkartenterminals, die über ein Kappmesser verfügen, um Abhörleitungen abzuschneiden. Möglich sind darüberhinaus drahtlose Verbindungen mit induktiver, kapazitiver, optischer oder funkgestützter Kopplung zwischen PET und Chipkartendummy, die dieses Problem vermeiden.

Oben bereits genannt wurde die Möglichkeit, das PET und das Anwendungsterminal direkt (ohne Verwendung eines Chipkartendummies) zu verbinden. Dabei kann von Schnittstellen Gebrauch gemacht werden, über die das PET ohnehin verfügt, oder es können zusätzliche Schnittstellen eingebaut werden. Auch bei einer direkten Verbindung zwischen PET und Anwendungsterminal kann diese leitungsgebunden oder drahtlos ausgeführt sein. Wie oben bereits erwähnt, ließen sich auf Seite des PET ohne zusätzlichen Aufwand bereits vorhandene Infrarot- oder Funkschnittstellen für diesen Zweck einsetzen. Diese direkte Verbindung des PET mit dem Anwendungsterminal hat den Vorteil, daß sie ohne Chipkartendummy und Chipkartenkontaktiereinrichtung im Anwendungsterminal auskommt; allerdings kann diese Direktverbindung nicht mit heutigen Anwendungsterminals zum Einsatz kommen, da diese über keine derartigen Schnittstellen verfügen.

Die Tatsache, daß bei allen genannten Verbindungsarten die Kommunikation zwischen PET und Terminal leicht abhörbar ist, stellt keinen Nachteil dar, da die Erfindung den Einsatz starker kryptographischer Algorithmen ermöglicht. Werden diese verwendet, spielt es keine Rolle, ob die Kommunikation abgehört werden kann, da die verschlüsselten Daten für den Angreifer wertlos sind.

Beim Einsatz des PET in Chipkartenanwendungen sind verschiedene Betriebsmodi denkbar:

1. Die Hauptanwendung ist der Einsatz als "Chipkartenersatz". Dabei tritt das PET (für das Anwendungsterminal) als Benutzertoken (Sicherheitstoken) mit Display und Tastatur auf. Das PET kann dabei zusätzlich über ein oder mehrere Sicherheitsmodule z. B. in Form einer Chipkarte verfügen, um sensitive Daten besonders zu schützen.
2. Der zweite Betriebsmodus ist notwendig für Diensteanbieter, die an konventionellen Chipkarten festhalten wollen oder müssen. Für solche Fälle kann das PET eine Visualisierungsfunktion bereitstellen. Die Chipkarte des Anwenders kann ganz normal in ein Anwendungsterminal eingesteckt und benutzt werden. Steht hingegen ein PET zur Verfügung, kann die Chipkarte auch in eine dafür vorgesehene Chipkarten-Kontaktiereinrichtung des PET eingeschoben werden. Das PET wiederum wird mit dem Chipkartenterminal verbunden. Auch hierbei kann das PET über ein oder mehrere Sicherheitsmodule verfügen, um · besonders kritische Daten besonders zu schützen.
Die Chipkarte arbeitet in diesem Modus wie vom Hersteller vorgesehen; das PET stellt lediglich die Verbindung zwischen Terminal und Chipkarte her. Dabei überwacht es die Kommunikation zwischen Chipkarte

und Terminal und visualisiert die durchgeführten Transaktionen für den Benutzer. Dabei sind drei verschiedene Varianten denkbar:

(a) Diese Variante bedingt, daß die Kommunikation zwischen Chipkarte und Anwendungsterminal nach einem Protokoll abläuft, welches ein Abhören der Kommunikation gestattet, ohne daß dadurch die Sicherheit der Anwendung beeinträchtigt würde. Das PET hört die Kommunikation mit und stellt die durchgeführten Transaktionen für den Benutzer dar.

(b) Diese, zweite Variante erlaubt eine vollständig verschlüsselte Kommunikation zwischen Chipkarte und Anwendungsterminal. Da diese nicht abgehört werden kann, muß einer der beiden Kommunikationspartner (also Chipkarte oder Anwendungsterminal) auf der Kommunikationsleitung zusätzliche Meldungen für das PET erzeugen, die von diesem dann visualisiert werden können. (Diese Meldungen müssen natürlich nur erzeugt werden, wenn tatsächlich ein PET zur Visualisierung vorhanden ist.) Im Normalfall sollten diese Meldungen allerdings von der Chipkarte generiert werden, da ein Benutzer üblicherweise eher dem Transaktionsterminal als seiner eigenen Chipkarte mißtrauen wird. Auch diese Meldungen können verschlüsselt werden, so daß lediglich das PET, nicht jedoch das Transaktionsterminal diese Meldungen lesen kann. Voraussetzung hierfür ist natürlich, daß die Kommunikation zwischen Kartenterminal und Chipkarte nicht durch die Kommunikation zwischen Chipkarte und PET gestört wird, da sie (zumindest bei Chipkarten nach heutigen Standards) über dieselben Kommunikationskanäle ablaufen muß.

(c) Die dritte Variante stellt eine Erweiterung der zweiten dar. Hier wird das PET nicht nur als Visualisierungsgerät verwendet, sondern auch als Eingabegerät. Die Chipkarte kann auch hierbei ganz normal in das Anwendungsterminal gesteckt und benutzt werden. Wird sie hingegen in einem PET betrieben, visualisiert das PET alle Transaktionen wie bei der zweiten Variante. Es kann aber auch als Eingabeterminal verwendet werden, etwa um Benutzer-Authentikationsgeheimnisse einzugeben. In dem Fall, da die Kommunikation zwischen PET und Chipkarte verschlüsselt abläuft, ergäbe sich der große Vorteil, daß das Anwendungsterminal das Benutzer-Authentikationsgeheimnis nicht ausspähen kann.

3. Der dritte Betriebsmodus könnte Transaktions-Journal genannt werden. In diesem Modus protokolliert das PET alle (ggf. während eines eingeschränkten Zeitraumes) durchgeführten Transaktionen, so daß der Benutzer z. B. nachvollziehen kann, wieviel Geld er wo mit welcher Kartenapplikation ausgegeben hat.

4. Der vierte Betriebsmodus ist eine Auskunftsfunktion. Hier können Daten von Speicherkarten angezeigt werden, z. B. wie hoch ist der Restbetrag auf einer Telephonkarte, welche Daten stehen auf einer Krankenversicherungskarte oder welcher Restbetrag ist noch auf einer Geldkarte verfügbar.

Literatur

[1] Effing, Wolfgang, und Rankl, Wolfgang: Handbuch der Chipkarten. 2. Auflage, Carl Hanser Verlag, München, Wien, 1996

[2] Schneier, Bruce: Applied Cryptography-Protocols, Algorithms and Source Code in C. 2nd edition, John Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore, 1996

[3] Schneier, Bruce: Angewandte Kryptographie-Protokolle, Algorithmen und Sourcecode in C. Addison-Wesley Publishing Company, Bonn, Reading/Mass., New York, 1996.

Patentansprüche

1. Portables, netzunabhängig betreibbares elektronisches Gerät, **dadurch gekennzeichnet**, daß es die typischen Funktionen eines Mobiltelephons, eines elektronischen Personal Organizers oder eines Taschenrechners etc. einerseits (im folgenden "Transaktionsgerät" genannt) und typische Funktionen von Chipkartenapplikationen andererseits vereinigt.

2. Gerät nach Anspruch 1 oder 1, dadurch gekennzeichnet, daß die Chipkartenapplikation(en) ganz oder teilweise Hard- und Software nutzt, über die das Transaktionsgerät ohnehin verfügt.

3. Gerät nach den Ansprüchen 1–3, dadurch gekennzeichnet, daß das Gerät über ein oder mehrere Sicherheitsmodule zur besonderen Sicherung kritischer Daten der Chipkartenapplikation(en) verfügt.

4. Gerät nach den Ansprüchen 1–3, dadurch gekennzeichnet, daß es die Kommunikation einer Chipkarte mit einem Anwendungsterminal visualisiert.

5. Gerät nach den Ansprüchen 1–3, dadurch gekennzeichnet, daß es als Ein- und/oder Ausgabegerät in einer Chipkartenapplikation verwendet werden kann.

6. Gerät nach den Ansprüchen 1–3, dadurch gekennzeichnet, daß es ein Journal aller mit diesem Gerät durchgeführten Chipkartentransaktionen führen kann.

7. Gerät nach den Ansprüchen 1–3, dadurch gekennzeichnet, daß es den Inhalt von Speicherchipkarten anzeigen kann.

8. Gerät nach den Ansprüchen 1–7, dadurch gekennzeichnet, daß es über eine Schnittstelle mit dem Transaktionsterminal verbunden wird, über die das Transaktionsgerät ohnehin bereits verfügt.

9. Gerät nach den Ansprüchen 1–7, dadurch gekennzeichnet, daß es über eine spezielle Vorrichtung ("Chipkartendummy" bzw. "Chipkartennachbildung") verfügt, mit deren Hilfe das Gerät mit einem Chipkartenterminal verbunden werden kann.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Verbindung zwischen der Vorrichtung und dem Gerät über metallische Leiter hergestellt wird.

11. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Verbindung zwischen der Vorrichtung und dem Gerät über Lichtwellenleiter hergestellt wird.

12. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Verbindung zwischen der Vorrichtung und dem Gerät drahtlos hergestellt wird.

13. Vorrichtung nach den Ansprüchen 9–12, dadurch gekennzeichnet, daß die Verbindung zwischen der Vorrichtung und dem Chipkartenterminal über metallische Kontakte hergestellt wird.

14. Vorrichtung nach den Ansprüchen 9–12, dadurch gekennzeichnet, daß die Verbindung zwischen der Vorrichtung und dem Chipkartenterminal kontaktlos hergestellt wird.

15. Vorrichtung nach den Ansprüchen 9–14, dadurch gekennzeichnet, daß die Vorrichtung selbst nicht über aktive elektronische Komponenten verfügt.

16. Vorrichtung nach Anspruch 9–14, dadurch gekennzeichnet, daß die Vorrichtung selbst über eigene aktive elektronische Komponenten verfügt.

17. Gerät nach Anspruch 1–17, dadurch gekennzeichnet, daß das Gerät die begrenzte oder vollständige Freigabe von Chipkarten-Transaktionen erlaubt, ohne mit dem Anwendungsterminal verbunden zu sein (Vorfreigabefunktion).

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 198 41 862 A1
Int. Cl.[7]: G 07 F 7/08
Offenlegungstag: 16. März 2000

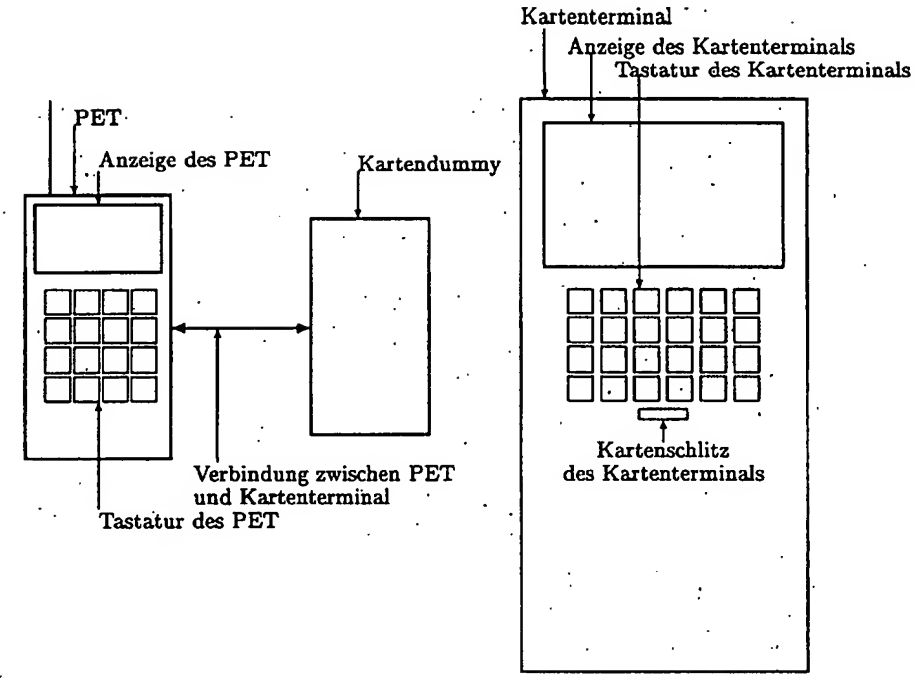

Abbildung 1: Verbindung zwischen PET und Kartenterminal mittels eines Chipkartendummies